

## REMARKS

Claims 1-72, 101 and 102 stand rejected on the ground of nonstatutory obviousness-type double patenting over claims 1-20 of U.S. Pat. No. 6,012,039.

Method claims 1-19, 25-38, 52-63 and 102 stand rejected under 35 U.S.C. § 101 as directed to nonstatutory subject matter.

Claims 1-72, 101-102 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Schockley et al. (U.S. 5,534,855), in view of Schultz et al. (U.S. 5,056,019).

Claims 1-72, 101 and 102 remain in the case for reconsideration.

Minor grammatical amendments are made to add commas to dependent claims. Dependent claims 29, 32, 38, 39, 51, 53, 59, 70 and 71 are amended to change language to be more definite and correct dependencies. Independent method claims are amended as discussed below to make the statutory subject matter more clear. Device claim 64 is amended to clarify the relationship of claim elements. Dependent claims 57 and 67 are amended to be more specific as to the successful match identifying the user and locating the rule module for that user, as supported by FIG. 2.

### Response to Nonstatutory Double Patent Rejection

Applicant is prepared to submit a Terminal Disclaimer to overcome the nonstatutory double patenting rejection over U.S. Pat. No. 6,012,039 once all the statutory grounds for rejection are overcome.

### Response to Nonstatutory Subject Matter Rejection

Applicant traverses the rejection under 35 USC § 101.

Under In re Bilski, 2007-1130 (Fed. Cir., October 31, 2008, en banc), the Court held at page 32 that "the applicable test to determine whether a claim is drawn to a patent-eligible process under § 101 is the machine-or-transformation test set forth by the Supreme Court and clarified herein...."

The Examiner acknowledges in para. 7 of the Action that this test provides two alternative ways (a) or (b) for a process to qualify as statutory under Section 101, concluding that "If **neither** of these requirements is met by the claim(s), the method is not a patent eligible process under 35 USC § 101." (Emphasis added)

In making the present Section 101 rejection, however, the Examiner states in paragraph 8 "In this particular case, the bodies of the independent claims do not recite any

particular apparatus that they are tied to." This rejection ignores the alternative "transformation" branch of the analysis, which will be discussed further below.

Independent method claims 1, 25, 54, 63 and 102 are amended to overcome the specific rejection made by the Examiner, namely to recite in the body of the claim specific apparatus that the method claims are tied to. The preamble of each such claim is amended, if not already recited, to state that the method uses a computer or computer system which includes the electronic identifier and electronic rule module clearinghouse. The body of each such claim is likewise amended to specify that the pattern data is stored in the computer in association with at least one execution command of the user. Further, the body of each such claim is amended to recite that the biometric samples are taken via a biometric sensor. Claims 1 and 25 are amended to state that a designated rule module is invoked by the electronic rule module clearinghouse, which is recited in the preamble as part of the computer. Claims 54, 63 and 102 are amended to specify that the computer performs the last step recited in each claim. Accordingly, all of the independent claims recite specific apparatus in the body of the claim that the method claims are tied to.

Additionally, the independent claims recite transformations of the type qualifying as statutory subject matter under In re Bilski and the authority cited therein. Taking claim 1 as exemplary, a biometric sample is taken from a user by a biometric sensor and registered in the electronic identifier. A later step takes a bid biometric sample from a user by a biometric sensor and compares it to the registered biometric sample in the electronic identifier. The taking of the biometric samples and input to the computer requires a conversion or transformation of the biometric samples (e.g., fingerprint, iris scan, retinal, etc.) from the particular form in which the biometric sensor detects the biometric sample -- for example, physical characteristics captured as a two-dimensional image -- into a digital format that can be stored and compared in the computer -- a binary character string or array. The comparison of the digitized biometric samples constitutes a further transformation, producing a successful or failed identification of the user -- an output from the electronic identifier saying who the user is. The successful identification leads to a further transformation in which the rule module of the computer is invoked to execute an electronic transmission -- an output of the execution command that is part of the rule module. The other independent claims contain essentially the same kinds of transformations.

The Court in Bilski explains the transformation part of the test, starting at page 24, last paragraph, and particularly with respect to computer-related inventions on pages 25-26, citing the example of In re Abele, 684 F.2d 902 (CCPA 1982). The Court sought to make

clear that the transformation was not limited to compositions of matter or material objects, stating on page 26 "We further note for clarity that the electronic transformation of the data itself into a visual depiction in Abele was sufficient; the claim was not required to involve any transformation of the underlying physical object that the data represented."

Under the Court's analysis in Bilski, the transformation described above with reference to claim 1 also qualifies the subject matter of that claim, and by extension the other independent method claims, as patent eligible under 35 USC § 101. As in Abele at page 26, in this case "the claimed process is limited to a practical application of a fundamental principle to transform specific data" namely, in terms of claim 1, taking biometric samples and comparison thereof, leading to an identification of a user, further leading to invoking of a rule module to execute an electronic transmission. Accordingly, the method claims in the present case recite statutory subject matter under 35 USC § 101.

#### Response to § 103 Rejection

Applicant traverses the rejection of the claims under 35 U.S.C. § 103 as unpatentable over Shockley in view of Schultz.

Other than again asserting the prior obviousness rejection, adding a few more citations to Shockley et al., the Examiner has not responded to the arguments Applicant submitted in the Amendment filed 28 May 2008. The action does not comply with MPEP 707.07(f).

The Examiner has again given a blanket rejection of claims 1-72 and 101-102, without any particularized reading of the claims on the references and reasons for the Examiner's conclusions. This rejection is not proper under 35 USC 103 and the controlling case law. In a prior case filed by Applicant, which was appealed, the Board reversed, holding that the Examiner had failed to establish a *prima facie* case under 35 U.S.C. 103. Ex Parte Hoffman et al, Appeal No. 2006-0464, decision mailed Aug 28, 2006, copy attached to Applicant's prior Amendment. As stated by the Board at pages 4-5:

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the examiner to establish a factual basis to support the legal conclusion of obviousness. See In re Fine, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). In so doing, the examiner is expected to make the factual determinations set forth in Graham v. John Deere Co., 383 U.S. 1, 17, 148 USPQ 459, 467

(1966). The examiner must articulate reasons for the examiner's decision.

In re Lee, 277 F.3d 1338, 1342, 61 USPQ2d 1430, 1434 (Fed. Cir. 2002). . . .

The examiner cannot simply reach conclusions based on the examiner's own understanding or experience - or on his or her assessment of what would be basic knowledge or common sense. Rather, the examiner must point to some concrete evidence in the record in support of these findings." In re Zurko, 258 F.3d 1379, 1386, 59 USPQ2d 1693, 1697 (Fed. Cir. 2001). Thus the examiner must not only assure that the requisite findings are made, based on evidence of record, but must also explain the reasoning by which the findings are deemed to support the examiner's conclusion....

In making the rejection, the Examiner lists the elements of claim 1 and cites Shockley at col. 5, lines 35-37; col. 3, lines 14-33, and col. 7, line 46, and Schultz col. 5, lines 2-7 as follows:

11. As per claims 1-72 and 101-102, Shockley et al. describes an invention comprising of:

a. ("a user registration step, wherein a user registers with an electronic identifier at least one registration biometric sample taken directly from the person of the user")--an applicant 100 supplies biometric information 105 to a registrar 110 as part of the processing of an account (C.5, LL. 35-37);

b. ("formation of a rule module customized to the user in a rule module clearinghouse, wherein at least one pattern data of a user is associated with at least one execution command of the user") (C9, L1-13);

c. ("a user identification step, wherein the electronic identifier compares a bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed identification of the user")--a user identification step, wherein the electronic identifier compares a bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed identification of the user (C8, L51-59 and C9, L12-13);

d. (“a command execution step, wherein upon successful identification of the user at least one previously designated rule module of the user is invoked to execute at least one electronic transmission; wherein a biometrically authorized electronic transmission is conducted without the user presenting smartcards or magnetic swipe cards”);

e. Authorization to execute any task is validated at the time a request is made by comparison of the digitized canonical forms of biometric data of the user completing the request with those of the user initiating the request (C. 3, LL. 14-33).

12. Shockley et al. did not explicitly describe an invention in which the process being validated is a reward program. However, Shultz describes a reward system in which the consumer is identified using a consumer identification code (C5, LL.2-7).

....

14. Shockley et al. describes a process, taking place in a wide area network (C7, LL. 46) ....

This rejection disregards several limitations of the independent claims, as well as the entire subject matter of most of the dependent claims. It also overlooks a number of aspects of the cited references that are contrary to the proposed combination. The foregoing rejection, therefore, fails to establish a *prima facie* case of obviousness under the controlling authority as cited above.

To make the analysis simpler, Applicant will focus on selected independent claims, and likewise on a sampling of the dependent claims. Claims 1-72 and 101-102 include six independent method claims -- 1, 25, 54, 63, 101 and 102. There are also two apparatus or system claims -- claim 20 directed to a system which supports the method of claim 1 and claim 64 which supports the method as defined in claim 54. We start with claims 54 and 64, which parallel claims 1 and 20 but in slightly broader terms:

54. A biometric method implemented in a computer system for processing electronic transmissions, comprising:

registering in the computer system at least one registration biometric sample taken directly from a user via a biometric sensor;

forming a rule module customized to the user in a rule module clearinghouse stored in the computer system, the rule module associating at least one pattern data of the user with at least one execution command of the user;

comparing a bid biometric sample subsequently taken directly from the person of the user via a biometric sensor with at least one previously registered biometric sample for producing either a successful or failed match; and

invoking the rule module of the user upon a successful match to execute at least one electronic transmission from the computer system.

64. A computer system device for biometric processing of electronic transmissions, comprising:

a biometric input apparatus, for providing a bid or registration biometric sample of a user;

an electronic rule module clearinghouse, having at least one rule module including at least one pattern data of the user associated with at least one execution command of the user;

an electronic identifier, to compare at least one registration biometric sample stored in the electronic identifier with a bid biometric sample to produce either a successful or failed match; and

a command execution module, responsive to a successful match to invoke at least one execution command in the electronic rule module clearinghouse to execute an electronic transmission.

It is readily apparent that these claims contain features not shown in the Shockley and Schultz references. Claim 54 (like claim 1, quoted in the Action at para. 11a) starts with a user registration step, which the Examiner correctly finds in Shockley at col. 5, lines 35-37.

The second element of claim 54 (also like claim 1) calls for "forming a rule module customized to the user in a rule module clearinghouse, the rule module associating at least one pattern data of a user with at least one execution command of the user." Action at para. 11b cites Shockley at col. 9, lines 1-13, but gives no reasoning as to why the cited teachings

supply this element. Nor does comparison of the cited text, as understood in the context of Shockley, as a whole, reveal teachings pertinent to the quoted element as understood in the context of claim 1 (or 54) as a whole.

The cited text (Shockley, col. 9, lines 1-13) only describes a set procedure for validating an account certificate obtained as part of a user login before proceeding with user authentication (See col. 8, lines 60-63). The cited text identifies why a request may fail, and then says:

“Only if the computer platform validates the credential and the request is authorized for the particular action are CBAD checks, if any, made. If either set of account credentials does not contain CBAD data. . .the approval entry is rejected and the process terminated. If both sets of account credentials contain CBAD data, then the digitized biometric data present in each set of account credentials are compared at step 164.” (col. 9, lines 4-13)

None of this pertains to or suggests the step in claim 54 (and claim 1) of forming a “rule module customized to the user. . .associating. . .pattern data of the user with at least one execution command of the user.”

The third element of claim 54 calls for a "comparing a bid biometric sample taken directly from the person of the user with at least one previously registered biometric sample for producing either a successful or failed match." The Examiner quotes a similar element of claim 1 in the Action at para. 7c and cites Shockley, col. 8, lines 51-59 and col. 9, lines 12-13. Deeper analysis shows that the claimed comparison is patentably distinct from that cited in Shockley. What are compared are the biometric data contained in two sets of account credentials, and that if the biometric data are similar the approval entry is rejected and the process is terminated. (Shockley col. 9, lines 14-18) As explained in col. 3, lines 14-25 and col. 5, lines 35-61, and summarized neatly in Shockley claim 1, elements A and D, the compared biometrics are both registered biometrics of a user, for different accounts. There does not appear to be any comparison in Shockley of a biometric taken at the time of attempted access to the system with a previously-registered biometric. In the words of claim 54 (and 1) as amended, Shockley does not teach comparison with the previously-registered biometric of a biometric sample that is subsequently taken from the user, i.e., when the user later tries to access the system to process an electronic transmission.

As explained at col. 3, lines 14-25, Shockley's system compares identification information stored in two different user accounts to determine whether the first account and the second account are aliases for the same user.

As further explained in Shockley col. 5, lines 36-58, each time a user sets up a new account, user biometric data is captured and stored in a certificate. When a user logs onto a workstation, as explained in col. 6, lines 21-25, the user inputs information such as user name that is used to fetch an account certificate as a first step in authenticating, or confirming the identity of the user. When requests are initiated from two accounts, ostensibly by the same user, under different aliases, this is detected in the procedure described at col. 8, line 30 to col. 9, line 18, by comparing the two certificates. "If the identification step identifies different user accounts, the two sets of account credentials are checked for the presence of CBAD data at step 162." (Col. 8, lines 51-53) "If both sets of account credentials contain CBAD data, then the digitized biometric data present in each set of the account credentials are compared at step 164." (Col. 9, lines 10-13).

Thus, the comparison in Shockley is of two previously-registered sets of biometrics. In Shockley's comparison, neither biometric is taken when the comparison is to be made; it is taken when the account is set up. In contrast, the comparison in claim 54 is of a bid biometric subsequently taken from the person of the user and compared to a previously-stored or registered biometric. Thus the third element of claim 54 is not taught by Shockley. The corresponding element of claim 1 is likewise not taught by Shockley.

The fourth element of claim 54 (and of claim 1) is not only not taught by Shockley but is taught away from by Shockley: "invoking the rule module of the user upon a successful match to execute at least one electronic transmission." The Examiner does not cite any part of Shockley for this teaching. Contrary to this recitation, Shockley teaches, at col. 9, lines 14-18, "If the compared digitized biometric data are within a predetermined range of similarity, the two sets of account credentials are presumed at step 169 to belong to the same user, and the approval entry is rejected and the process terminated."

Shockley describes an example of how his method can be used to prevent fraudulent approval of an expense report commencing at col. 9, line 36 and continuing through col. 12. Summarizing, an individual can fill out and submit an expense report through the Shockley system. The expense report must be approved before it is forwarded to disbursements for a reimbursement check. The essential separation of duties requirement is that no individual can approve his own expense report. Each individual user can submit an expense report logged in under his own personal account and the expense report is posted in a queue where it is



retained for review. One or more individuals are given “management accounts” authorized to review and approve or reject expense reports. The request to approve the expense report created by the individual user triggers the certificate-based alias detection method. Each account certificate identifies the user and contains relevant information about each individual including digitized canonical biometric data for the individual (i.e., registration biometric data). As explained in col. 11, line 49, through col. 12, when a second user attempts to approve the expense report, the account certificate (CBAD data) for that user is verified and only then the digitized biometric data for each are compared for similarity. In contrast, the claimed method compares a bid biometric to a previously-registered biometric is used to identify the user at the time of attempted access, before accessing the rule module customized to the identified user. (See Shockley, col. 6, lines 44-47: “At no time during the authentication process is the CBAD data in the account certificate used. Since CBAD data does not determine the success or failure of a login authentication, . . .”)

If the two previously-registered biometric data are regarded as identifying the same user, the application server system 116 must assume that the two users are in fact the same individual even though the corresponding account certificates belong to distinct accounts, and the expense report approval is blocked. Thus, Shockley teaches a one-to-one comparison of two previously-registered sets of biometric data. And Shockley terminates the user’s attempted access upon a successful match (See Shockley, FIG. 3, col. 9, lines 10-18), directly contrary to the claimed invention.

The parts of Shockley cited in the preceding paragraphs also contradict the Examiner’s misinterpretation of col. 3, lines 14-33 in the Action at para. 11e. (See Shockley, col. 6, lines 44-47 quoted above).

Schultz is not cited for any of the foregoing teachings of claim 54 (or claim 1) missing from Shockley, either in regard to the rule module, its contents or its operation, or in regard to the capture and comparison of registration and bid biometric samples.

Accordingly, claim 54 is patentable over the Shockley and Schultz references.

System claim 64 is likewise patentable over Shockley and Schultz.

Claim 1 recites the method as recited in claim 54 with some added limitations including the further limitation that the recited method is “tokenless” as expressed in the preamble of claim 1 as well as in the final element of claim 1. System claim 20 recites the system as recited in claim 64 with some added limitations including the further limitation that the recited method is “tokenless.” Based on the foregoing discussion of claims 54 and 64, claims 1 and 20 should also be patentable over Shockley and Schultz.

The additional "tokenless" feature recited in the preamble and again in the last element of each of claims 1 and 20 was held to be a patentable distinction in the above-identified Board decision. It likewise constitutes a patentable distinction -- in addition to those discussed above -- over the Shockley and Schultz references. Both Shockley and Schultz call for the use of a token. In Shockley "The private key is issued to the user (typically in the form of stored information in some device 115 such as a pass card)..." (Col. 5, lines 49-51) or in a smartcard (Col. 6, lines 34-37). Schultz calls for encoding or imprinting the consumer ID code in a member identification card, UPC bar-coding, or a magnetic stripe of a debit card. (Col. 6, lines 31-53). Thus, both Shockley and Schultz describe token-based method and apparatus, contrary to claims 1 and 20.

Accordingly, claims 1 and 20 are additionally allowable based on the tokenless distinctions discussed above.

Method claim 63 covers a more elaborate version of the method of claim 54. It contains essentially the same features of claim 54 but further specifies a primary and a secondary user with registration of biometric samples for each and with respectively associated primary and secondary rule modules, subordination of the secondary rule module to the primary rule module, and a comparison of the bid and registered biometrics of the second user to invoke the primary user rule module. None of this is taught or suggested by the Shockley and Schultz references.

Method claim 25 is similarly directed to a method involving primary and secondary users, in somewhat more detail than claim 63. Claim 25 is allowable for the same reasons as claim 63. Additionally, claim 25 contains the "tokenless" feature discussed above, and so should also be allowable on that basis.

Claims 101 and 102 are directed to methods of operation of the invention where there is already a registered biometric of the user in the system. Claim 102 is directed to the operation of the rules module clearinghouse responsive to the match of a bid biometric with the registered biometric to extract data associated with the user and pertinent to the rule module and performing an action with the extracted data that is defined by the rule module. This sequence is not taught or suggested by the Shockley and Schultz references. Claim 101 similarly starts by matching the biometric sample from the user with a registered sample, then transmitting an access key to the user terminal, receiving a request to validate the access key from a third party location and, if the validity of the access key is confirmed, transmitting user's account access information to the third party location or computer. This sequence also is not taught or suggested by the Shockley and Schultz references. Accordingly, the

Examiner's blanket rejection of all the claims fails to establish a *prima facie* case of obviousness with respect to claims 101 and 102.

The foregoing analysis demonstrates why the independent claims are allowable over the Shockley and Schultz references. The dependent claims are not separately rejected. Indeed, they claim additional features further limiting the allowable independent claims, not taught or suggested by the Shockley and Schultz references. A sampling of the dependent claims is indicative.

For example, claims 2 and 21 provide for the command execution module to communicate with third-party computers, similarly to claim 101.

Claim 7 provides an alert if a user attempts to re-register and the new registration sample matches the previous registration sample. Shockley allows a user to register in multiple accounts as further explained in Shockley col. 5, lines 36-58, and then provides a method, discussed above, at col. 9, lines 14-18, preventing the requested access or action.

Claims 9 and 10 provide for a personal ID code and provide a theft resolution step to change that code if the biometric sample has been fraudulently duplicated.

Claims 26-29, 40-42, 59, 70 and 71, among others, claim various specific applications of the user profile and execution commands to control access to various goods and services, such as insurance benefits and purchase of restricted goods such as alcohol and tobacco. Claim 62 specifically calls for the pattern data to include demographic data about the user and the execution command determines eligibility of the user to access goods, data or services.

Claims 37, 38, and 50 provide execution commands for controlling access of a subordinated user, as determined by a primary user.

Claim 44 further specifies a device in which a rule module includes at least one pattern data associated with two execution commands, and at least one execution command associated with at least two pattern data.

None of these features appear to be taught or suggested by the Shockley and Schultz references. Nor has the Examiner cited the Shockley and Schultz references specifically against these claims. Accordingly, the dependent claims are allowable in their own right as well as because the claims from which they depend are patentably distinct from the Shockley and Schultz references.

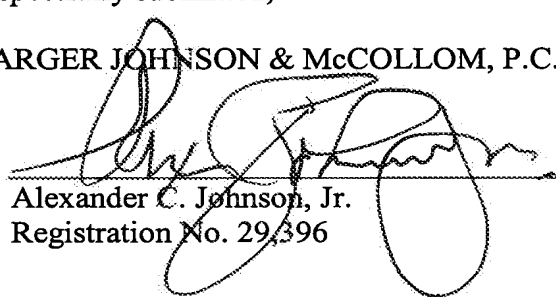
In view of the foregoing and the fact that the claims are otherwise allowable, the application should now be in condition for allowance. If any questions remain, the Examiner is requested to call the undersigned.

**60460**  
**Customer No.**

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

By

  
Alexander C. Johnson, Jr.  
Registration No. 29,396

210 S.W. Morrison Street, Suite 400  
Portland, Oregon 97204  
Telephone: (503) 222-3613